Immaterial Transfers with Material Consequences

By
Roland L. Trope
Trope and Schramm LLP

[We would like to thank the *Digital Protection* magazine for allowing us to reprint this article.]

Companies often perceive U.S. laws as bewildering in their complexity, burdensome in their compliance costs, and intimidating in the severity of their penalties. Particularly onerous is the defense trade controls regime embodied in the *U.S. International Traffic in Arms Regulations* (ITAR). The risks of noncompliance with ITAR appear in settlements reached in March 2006 between the U.S. State Department's Directorate of Defense Trade Controls (Directorate) and The Boeing Company and L-3 Communications (together with its subsidiary, Goodrich). These companies agreed to pay civil penalties of U.S. $15 million and $7 million, respectively, and to implement costly compliance improvements. Many companies discover only belatedly that an effective ITAR compliance program generates substantial commercial benefits. For example, if a U.S. firm plans to develop and sell a high-tech product to overseas commercial customers and does not realize that its proposed product will incorporate ITAR - controlled components, it could discover after significant development and testing expenditures that it cannot export the product to customers in certain countries (directly or indirectly) because the Directorate will not grant it a license. The company might also be prohibited from distributing the product's marketing materials to foreign nationals if such materials contain ITAR-regulated data, or from providing repair and maintenance services for such product to certain countries.

The risks of ITAR violations continue to increase with the proliferation of new communication technologies because companies fail to focus sufficiently on controlling their data and adverting the ways in which they often lose control of it. It is imperative that defense contractors retain tight control of digital data because the ITAR regulates data exports not only in hard copy but also in digital form (which is far easier to lose control of and with more serious consequences). Existing regulations already contemplate "immaterial" exports (including digital data) because the ITAR covers exports of data carried in the mind's eye. The act of showing a defense article's blueprints to a foreign national, for example, is deemed an immediate "export" to his or her home country.[1] The same ITAR provision regulates digital transmittals to a foreign national as if they were transfers of hard copies by hand. Moreover, without a license from the Directorate, a U.S. company cannot release ITAR-regulated data to any of its foreign national employees, whether such release occurs via the internet to an overseas location or via e-mail, instant messaging, or even file transfers through the company intranet to such employees located in the U.S. Companies intent on winning defense contracts or performing work subject to the ITAR must therefore fundamentally re-think their approach to technical data because the ITAR requires that they control the destinations of their digital transfers, internet broadcasts, and other electronic communications.

To assist in understanding the ITAR as they apply to digital data, we explore the missteps of a hypothetical company, NanoNautica, as it embarks on defense contracting for the U.S. government.

1. *Code of Federal Regulations*. Title 22, Section 120.17(a)(1), 2005.

The Company

NanoNautica, a U.S. corporation, earned a significant market share for its advanced design of high performance, computer-controlled precision instruments. Headquartered in Cupertino, California, NanoNautica claims no national corporate identity, has satellite offices in Brazil, the Netherlands, Norway, and China, and employs several Indian and Iranian nationals as software programmers, as well as a Brazilian national as its information technology (IT) administrator. In this respect, it is not dissimilar from many other modern multinational corporations (MNCs). Until 1992, NanoNautica was a U.S. defense contractor, but frustrated by disagreements with the U.S. government over rights to its technical data, its board of directors approved the sale of its defense unit and redirected production towards civil aeronautics. After the September 11, 2001 attacks, however, its management was attracted by the financial opportunities in the U.S. Department of Defense (DoD) and NASA contracts and ordered modifications of two products for sale specifically to those customers. Company engineers adapted a control movement gyroscope (CMG) and related software to facilitate guidance of a craft's orientation that outperforms CMG systems currently deployed on U.S. spacecraft. NanoNautica also modified for military use its commercial gyro microchip–a device that determines an airborne plane's orientation, or helps to stabilize and steer guided missiles.

International Traffic in Arms Regulation Compliance Planning

As the person in charge of NanoNautica's data governance procedures, your responsibilities include ensuring company-wide compliance with all regulations covering the export of defense articles, services, and technical data. The company's chief information security officer (CISO) asks you to assist her in preparing for a meeting with the chief executive officer (CEO). Her list of potential ITAR compliance issues includes:

- **Perimeter defenses**. NanoNautica will consolidate its defense-related work into its Cupertino plant and reinforce the perimeter and entrance safeguards. The CEO believes this will avert any noncompliance with the ITAR.
- **E-mail and instant message access.** NanoNautica's IT administrator (resident in its Sao Paulo office) has access privileges to all international communications (including e-mail and internal messages discussing and transmitting technical data related to the CMG and gyrochip projects). Management instructed engineers on those projects to use code names for e-mail attachments containing sensitive data, believing that this routine, low-cost way of disguising sensitive data would minimize the risk that anyone outside the defense unit with access privileges would open such attachments – a questionable assumption. In practice, the engineers regularly selected constellation names for CMG files and names of stars for gyrochip files – an all transparent pattern that could facilitate data leaks.
- **Network security.** To ensure the control of the destinations of ITAR-regulated data transmissions, NanoNautica's legal counsel proposed that the company create a special access-controlled intranet solely for CMG and gyrochip communications. Such a network, however, would be costly to create and maintain, and could diminish the productive brainstorming among engineers that often leads to innovative engineering solutions. The IT department responded with a counterproposal: encrypt all sensitive traffic, and distribute the key to authorized personnel with instructions to treat it as a "trade secret." If the company adopts that proposal, the CEO prefers to encrypt only the attached, code-named files; while this solution has the advantage of fixing the cost of securing relevant files, it ignores the problems that arise when individuals must make ad hoc decisions as to which files contain ITAR-regulate data. It also

overlooks known encryption risks.[2] Moreover, all relevant personnel must be trained in ITAR compliance, ultimately a much more costly solution than omnibus encryption. Ad hoc decisions–even with compliance training–pose a significant compliance risk because they decentralize compliance authority and diffuse control.

- **Laptop use.** There are certain hours when all NanoNautica engineers worldwide can work collectively on problems from their offices or homes. This requires NanoNautica to issue company laptops to facilitate communications. ITAR-controlled data on these laptops makes them inviting targets for theft by competitors and intelligence agents (both military and corporate). Companies in comparable fields with similar information security risks bar personnel from using laptops, despite frequent travel, because theft would pose unacceptable risks. Their policy is simple: "The best laptop for us is no laptop at all."[3] NanoNautica is considering the efficacy of such a policy for its CMG and gyrochip project engineers, as well as practicable and less Draconian alternatives.

Because the CEO wants to recommend to NanoNautica's board of directors an omnibus program that addresses both compliance and security issues, there is potential accountability for you and the CEO in the event of a compliance oversight or breakdown. Your responsibility is to design a compliance program that effectively balances costs and risks, yet avoids the strategic error most compliance officers make at this phase: designing a program that responds to corporate officers' wishes rather than to the applicable regulations (in this case, ITAR requirements and their probable interpretation by the Directorate).

The *International Traffic in Arms Regulation*

After conducting an audit of company action (and inaction) with respect to ITAR requirements, you identify several areas in which the company must make changes to comply with ITAR.

Registration

The ITAR requires any company engaged in the manufacturing or exporting of defense articles or the furnishing of defense services in the U.S. to register with the Directorate.[4] A single instance of manufacturing a defense article triggers this duty. NanoNautica should therefore have registered with the Directorate before it began production of articles developed, adopted, or modified for defense use (such as the CMG and modified gyrochip)[5].

Accountability

The ITAR required companies to appoint an empowered official who must sign the registration form filed with the directorate.[6] The ITAR further requires that the empowered official have "independent authority" to enquire into any aspect of a proposed export." To verify the legality of the transaction and the accuracy of the information to be submitted" to the Directorate, and to refuse to sign any license application or other request for approval without prejudice or other adverse

---

2. *Federal Financial Institutions Examine Council, IT Examinations Handbook*: Information Security, July 2006, pp. 56-57; www.ffice.gov/ffiecinfobase/booklets/information_security/information_security.pdf.

3. V. Vara, "Moving Targets: How Companies Can Keep Employees from Losing the Information in Their Laptops," *The Wall Street Journal*, June 19, 2006, p. R9.

4. *Code of Federal Regulations*, Title 22, Section 122(a), 2005.

5. *Code of Federal Regulations*, Title 22, Section 122.21(a), 2005.

6. *Code of Federal Regulations*, Title 22, Section 122.25, 2005.

recourse."[7] These provisions create potential liability for the company and the empowered official, if the company commits certain ITAR violations.

It is the empowered official's responsibility to alert the company to "red flags" and to investigate any potential ITAR violations. The empowered official must also notify the Directorate within five days of any change in a company's ownership or leadership, an acquisition or divestment of a foreign subsidiary, a change in location (the consolidation of defense work in NanoNautica's Cupertino office) or a change in business (for example, if NanoNautica starts dealing "in an additional category of defense articles or defense services," which happened when it switched to making gyrochips for military systems).[8] In light of these requirements, NanoNautica is already in noncompliance with ITAR notification requirements.

Unlicensed Release of Technical Data

Companies should also be alert to the fact that, under the ITAR, "a license is required for the oral, visual or documentary disclosure of technical data by U.S. persons to foreign persons,"[9] as can occur when a firm responds to a foreign customer's request for a proposal or sends promotional product information to foreign national representatives of a U.S. or overseas firm. The ITAR requires a license for such exports "regardless of the manner in which the technical data is transmitted" (for example, in person, by telephone, electronic correspondence, and so on). It thus includes any and all data transmitted by e-mail, intranet, or instant message–regardless of whether the foreign recipient is outside or within the U.S. If a U.S. person transmits ITAR-regulated technical data by e-mail or instant message to a foreign national without a license, or enables a foreign national to obtain a copy of such data via such a transmission, an illegal export or release has occurred. Any compliance plan must therefore avert unlicensed releases of ITAR-regulated technical data to foreign nationals or to overseas officers, and recognize that for such a release to occur, a foreign national would not have to read an e-mail or even open its attached file.

In the digital era, this explanation seems counter intuitive. Surely the ITAR's provisions have evolved to conform to the reality of the ways MNCs do business using the internet and web sites to enable companies to work across national borders. NaonNautica's development of CMG units and gyrochips resulted from collaborative efforts by engineers from all its offices. Personnel around the globe routinely shared their ideas through the company's intranet, e-mail, instant messaging, and video conferencing using a voice-over-IP (VoIP) system. Thus, ITAR-controlled technical data related to CMGs. gyrochips, and software has been circulating in and out of the U.S. and between U.S. citizens and foreign nationals within the Cupertino defense plant throughout the research and development process. These routine transmissions, however, raise significant issues under the ITAR.

Deemed Exports of Data

Unlicensed transmissions of ITAR-controlled data from NanoNautica's Cupertino office to an overseas office are viewed as illegal exports, and each transmission is a separate violation. Additionally, each transmission of ITAR-controlled data from a U.S. person to a foreign national within the Cupertino location constitutes an unlicensed "deemed export" to that foreign national's country and is therefore a separate violation.

A question that frequently arises is whether there is a way to recharacterize company conduct to bring it within what is permissible under the ITAR. Does encryption, for example, avoid liability by

7. *Code of Federal Regulations*, Title 22, Section 120.25(4), 2005.

8 *Code of Federal Regulations*, Title 22, Section 122.4(a)(2), 2005.

9. *Code of Federal Regulations*, Title 22, Section 125.2(c), 2005.

making the transmission a non transfer? Can a recipient be described as possessing data only after it has been decrypted? The simple answer to both is "no".

The logic might not seem sound, but it is in fact the logic of ITAR, which defines "export" much more broadly. Companies subject to the ITAR must distinguish between procedures that retain control over data and procedures that relinquish control. Security protocols (such as encryption) that travel with sensitive data inevitably relinquish control of digital data to the recipient, whereas security protocols that limit who can handle and receive sensitive files retain control of digital data.

Files need not be decoded to violate the ITAR's prohibitions. Under ITAR, when a foreign national has an opportunity to obtain a copy of data, access is deemed to have occurred, even if the data is encrypted and purportedly unreadable. In the ITAR, such potential access constitutes an export and requires a license or exception from the license requirement. NanoNautica's IT administrator in its SAO Paulo office has access privileges to all internal communications including e-mail and instant messages discussing and transmitting data related to the CMG and gyrochip projects. Such access means that unlicensed transfers of ITAR-controlled data come within his review and thereby violate the ITAR.

Although NanoNautica's CEO prefers to encrypt ITAR-controlled e-mail, that is not enough to comply with ITAR because encryption could fail to provide a durable safeguard. A safer policy would be to adopt the proposed access-controlled intranet. It is important to recognize that the most obvious approach to portable security–encryption–is only a temporary stopgap. Placing encrypted, ITAR-controlled data in the hands of foreign nationals, in the absence of a license, removes the data from company control and places it in the control of those who might have a strong incentive to appropriate it. A compliance program cannot be characterized as effective if it relies solely on one safeguard or protocol to protect against unauthorized or unlicensed releases. Like a raccoon trying to rifle through a closed garbage can, a determined hacker (with enough computer power) can be counted on to crack encryption if he plays with it long enough.

If NanoNautica stores ITAR-controlled data in an unlocked closet in its Cupertino office and allows foreign nationals visiting from China to store briefcases in that closet, that would give them access to the ITAR-controlled data. This might seem to confuse access with disclosure. However, the ITAR's broad definition of export includes "disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad."[10] If a U.S. person transmits ITAR-controlled technical data by e-mail or instant message to a foreign person, or makes it possible for a foreign person to obtain a copy of such data by such transmission, an export has occured. Without a license, that export violates the ITAR. The ITAR does not define "export" to mean transfer and disclosure–transfer by itself is sufficient.

Penalties and Precautions

The magnitude of ITAR penalties makes compliance an extremely important data–governance issue. If the Directorate determines that such violations were unintentional, it can impose a civil penalty of up to $500,000 for each violation. One day of heavy e-mail traffic could expose NanoNautica to tens of millions in fines. And this does not illustrate merely a worst-case hypothetical. The Directorate routinely charges multiple violations. If it determines that the violations were intentional, the exposure is much greater: criminal penalties can be imposed of up to $1 million per violation or twice the amount NanoNautica might have gained from such conduct, whichever is greater. Moreover, whether civil or criminal, such violations result in strict liability–with no exoneration for good faith or inadvertence.

10. *Code of Federal Regulations*, Title 22, Section 120.17(a)(4), 2005.

A company's data governance policies must, therefore, ensure that its convenient conveyances of sensitive digital data do not result in ITAR violations, and thereby incur costly and disruptive internal investigations, negotiations with the Directorate, penalties, potential debarment from government contracts, and reputational damage (this last can be significant).

Lessons Learned

The ITAR is designed to protect the most sensitive data–military crucial to national security from release to actual or potential adversaries. If such a release occurs, NanoNautica will either be viewed as having given a foreign power the opportunity to appropriate ITAR-controlled data (probably aggravating its penalties) or as having created define-in-depth controls for its sensitive data that require a commensurate effort to circumvent (possibly mitigating its penalties).

NanoNautica should revise its original compliance program on a through internal investigation that identifies all potential ITAR noncompliance issues. It should then draft a plan for voluntary disclosure to the Directorate. NanoNautica might call a temporary halt to its defense work–a stand-down to permit the implementation of procedures that will prevent further unlicensed exports and "deemed exports."

Consolidation of defense work in one plant will not suffice. If NanoNautica wants to continue its collaborative mode of research and development, it must obtain licenses for each foreign recipient of ITAR-controlled data. The directorate, however, might not grant all the licenses NanoNautica seeks. Although it would be costly. NanoNautica should create a separate channel of communications for ITAR-controlled data, and should limit access to that channel to U.S. persons and ITAR-licensed foreign nationals.

NanoNautica should also encrypt all sensitive portable files (which might limit the damage caused by a violation by making it harder to break into and read the sensitive data.) And, it should train its engineers to alert it to proposed product developments that would require generation of, access to, or incorporation of ITAR-controlled data or technology. Such notice should enable NanoNautica to weigh the risks of pursuing such development in light of the possibility that the Directorate might not issue a license for sale to certain countries and their nationals.

The consequences of failing to recognize when a product incorporates ITAR-controlled data or technology can be glimpsed in an internal e-mail that the senior contracts manager at an L-3 subsidiary sent (after learning of unlicensed releases of certain gyrochips known as QRS-11 Sensors):

> BEI [a supplier of gyrochips] has confirmed that all QRS-11 Sensors, regardless of whether or not they are used predominantly for commercial applications are on the munitions list. This would mean that if we can't get a commodity, jurisdiction from the Department of State, which determines . . . [our avionics product] to be a commercial unit, we will need to have a validated license each time we export it, as well as having to submit a voluntary self disclosure for previously exporting it without a license. Obviously, we don't want that to happen.[11]

With each new technological enhancement of data mobility comes increased ways for sensitive data to leak. Daily CD burning and transmittals of electronic dispatches can create instant and specific exceptions to company's well intentioned compliance plan. Although no company can guarantee that its sensitive data will be secured against access by prohibited persons, companies should not let the conveniences of new technologies make ITAR-controlled data or any sensitive data–less secure.

---

11. Undated internal e-mail from L-3 subsidiary Goodrich Avionics, as quoted in *U.S. Department of State, Bureau of Political-Military Affairs Directorate of Defense Trade Controls, Draft Charging Letter* re: Investigation of Goodrich Corporation and L-3 Communications Corporation, pp. 6-7; www.pmdtc.org/Consent%20Agreements/2006/Goodrich%20Corporation/Draft%20Charging%20/Letter.pdf.

Companies should, therefore, routinely evaluate their compliance program's potential vulnerabilities as technology evolves. Companies can minimize the risk of inadvertent transfers of sensitive data without compromising research and development flexibility, if they tag data that has commercial value and legal sensitivity and control it accordingly. A conscientious program will significantly minimize (through not altogether eliminate) the risk of unauthorized access.

About the Author

Roland L. Trope is a partner in the New York City office of Trope and Schramm and an adjunct professor in the Department of Law, U.S. Military Academy. He provides strategic and legal advice on mergers and acquisitions, export and defense trade controls, trade sanctions, anti-money laundering, personal data protection, information security, intellectual property, cyberspace law, and defense procurements. He has a BA in political science from the University of Southern California, a BA and an MA in English language and literature from Oxford University, and a JD from Yale Law School. He coauthored the treatise Checkpoints in Cyberspace: Best Practices for Averting Liability in Cross-Border Transactions (American Bar Association, 2005). Contact him at e-mail address: roland.trope@verizon.net.